## REMARKS

This Application has been carefully reviewed in light of the Office Action mailed November 23, 2004 and the Advisory Action mailed February 8, 2005. Claims 1-6, 8-30, and 32-45 are pending in the Application. The Examiner rejected Claims 1-6, 8-30, and 32-45. Applicants have amended Claims 1, 2, 10, 14, 25-26, and 38. Applicants submit that no new matter has been added with these amendments. As described below, Applicants believe all claims to be allowable over the cited references. Therefore, Applicants respectfully request reconsideration and full allowance of all pending claims.

**Section 103 Rejections**

The Examiner rejects Claims 1, 11-13, 35-37, and 43-45 under 35. U.S.C. § 103(a) as being upatentable over U.S. Patent No. 5,455,855 issued to Hokari ("*Hokari*") in view of U.S. Patent No. 6,564,261 issued to Gudjonsson et al. ("*Gudjonsson*") and in view of U.S. Patent No. 6,389,462 issued to Cohen et al ("*Cohen*"). The Examiner rejects Claims 2-6, 8-10, 14-30, 32-34, and 38-42 under 35. U.S.C. § 103(a) as being upatentable over *Hokari* in view *Gudjonsson*. Applicants appreciate the Examiner's consideration of the application. Applicants respectfully submit, however, that the proposed combinations fail to disclose, teach, or suggest the elements recited in Applicants' claims.

As one example, Applicants submit that the *Hokari-Gudjonsson-Cohen* combination does not disclose, teach, or suggest "monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network," as recited in Applicants' independent Claim 1. In the Office Action, the Examiner acknowledges that *Hokari* does not explicitly disclose monitoring the type of streaming. (Office Action, page 3). Rather, the Examiner relies on *Gudjonsson* for disclosure of the recited features. With respect to *Gudjonsson*, the Examiner states that the reference discloses the "monitoring of all types of streaming." (Office Action, page 3). The portions of the reference relied upon by the Examiner, however, merely disclosed a registration system for a network that results in "messages [that] are not sent directly between users, but instead through at least one intermediate routing service (RS) provided on a server of one of the users" on the network. (Abstract). The routing service allows a user to "hide or mask his/her personal information from other users even when communicating with them." (Abstract). Accordingly, "a user may establish a communication session with another user without knowledge of the client device (e.g., PC, mobile phone, etc.) being used by the other user." (Abstract). Thus, the network enables communication services and the "initiating user need not know whether the other user is currently online via his/her PC or may instead be reached via page or mobile phone." (Abstract).

The network disclosed in *Gudjonsson* uses "smart routing . . . based on the user's currently active profile" to route an incoming communication to an appropriate client device. (Column 32, lines 63-64). This "basically means that whenever another specific user tries to contact the user using a specific mode of communication that user will be routed to a conversation endpoint or a message repository which can handle that mode of communication." (Column 32, line 64 through Column 33, line 1). "Based on settings in the profile, the other user could be routed to an auto-replier which responds that the user doesn't like him and doesn't want his calls, or be put through to the user's GSM etc." (Column 33, lines 1-5). Thus, *Gudjonsson* is limited to a network for routing incoming communications to an appropriate device based upon the type of communication. The disclosure of *Gudjonsson* is focused on the set up of the communication as it is initially received.

With respect to the portions of the reference relied upon by the Examiner in the Advisory Action mailed on February 8, 2005, Applicants respectfully submit that these portions also do not disclose, teach, or suggest "monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network," as recited in Applicants' independent Claim 1. Specifically, the portions disclose:

- That a user "can monitor the status of different contact users." For example, a user can monitor whether a contact user is logged on or off. Accordingly, "[w]hen the contact user $B_1$ comes online, the [user server] of user $B_1$ sends $B_1$'s online status to all [connection servers] 21 subscribed." (Column 27, lines 32-35).

- That a log of relevant events may be kept by the system in database 13. The types of events "fall into two main categories: events that are of interest to the administrator, and events that can be used for billing. For each event, the date and time of the event are stored, as well as which user was responsible for the event." For example, a log may be maintained to "see which user accounts have unsuccessfully attempted to authenticate themselves more than once or twice in a row, count the number of users who were logged in at a certain time or over the whole day, or to see which events took place just before and at the time the system crashed." (Column 31, lines 20-42).
- That "Connection Servers lie on the boundary between the unsecured Internet and the secure Intranet" and "function like firewalls of sort." Similar to above, Connection Servers "are able to log every connection and connection attempt. Log entries include such information as the date and time of day of the connection attempt, source IP number, user ID used for any authentication attempts and the reason for authentication failure." In certain embodiments, it is preferred that the Community Operator filters and audits traffic from the Internet destined for the Connection Servers to prevent hacking and to keep track of any hacking attempts." (Column 32, lines 27-48).
- That the "client-side application can work through a SOCKS firewall without the system administrator needing to do nay special setup, and through other firewalls by having the system administrator open a very limited number of ports." (Column 38, lines 33-38).

The maintaining of an event log, the monitoring of login status by users, and the use of a firewall, as disclosed in *Gudjonsson*, are very different from the features recited in Claim 1. Certainly these functions do not result in the monitoring of "communications transmitted . . . to ensure that the communications are media streaming to maintain the integrity of the trusted network," as recited in Claim 1. Rather, the functions of the system of *Gudjonsson* merely operate to identify and prevent hacking to the system. Furthermore, with respect to communications security, *Gudjonsson* discloses that "in certain embodiments of this invention all communications between a client and the [connection server] are secure" and that "[a]s for server-server communications, the network that handles communications . . . is assumed secure and protected." (Column 31, line 60 through Column 32, line 5). Thus, at least one passage relied upon by the Examiner teaches away from "monitoring communications . . . to maintain the integrity of the trusted network. For at least these reasons, Applicants respectfully submit that the recited features and operations are completely absent from the teachings of *Gudjonsson*.

For at least these reasons, Claim 1 is allowable over the cited references. Therefore, Applicants respectfully request reconsideration and allowance of Claim 1.

Independent Claims 2, 14, 26, and 38 recite limitations that are similar, though not identical, to the limitations discussed above with regard to Claim 1. As just one example, Claim 2 recites "monitoring communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network." Again, the Examiner relies upon *Gudjonsson* for disclosure of the recited features. With regard to similar features recited in Claim 1, Applicants have demonstrated above, however, that *Gudjonsson* does not disclose, teach, or suggest the recited features. Rather, *Gudjonsson* is limited to a network for routing incoming communications to an appropriate device based upon the type of communication. The disclosure of *Gudjonsson* is focused on the set up of the communication as it is initially received. Although *Gudjonsson* disclose the maintaining of an event log, the monitoring of login status by users, and the user of a firewall, these functions do not result in the monitoring of "communications transmitted between the untrusted device and the trusted IP telephone on the telecommunication link to ensure that the communications are media streaming to maintain the integrity of the trusted network," as recited in Applicants' Claim 2. Rather, the functions of the system of *Gudjonsson* merely operate to identify and prevent hacking to the system. Accordingly, for reasons similar to those discussed above with regard to Claim 1, Applicants respectfully submit that the references relied upon by the Examiner do not disclose, teach, or suggest each and every element as set forth in Applicants' independent Claims 2, 14, 26, and 38.

Dependent Claims 3-13, 17-25, 27-37, and 39-45 depend from Claims 2, 14, 26, and 38, respectively, which Applicants have shown above to be allowable. Dependent Claims 3-13, 17-25, 27-37, and 39-45 are allowable over the prior art of record at least because of their respective dependencies.

Additionally, dependent Claims 3-13, 17-25, 27-37, and 39-45 recite limitations that are not disclosed, taught, or suggested by the prior art. As one example, Claim 9 recites "monitoring the telecommunication link to determine whether the telecommunications being sent by the untrusted device use an appropriate audio format." Claim 24 recites similar, though not identical, features and operations. As a further example, Claim 10 recites "wherein monitoring the communications transmitted between the untrusted device and the trusted IP telephone comprises monitoring the telecommunication link to determine whether the telecommunications being sent by the untrusted device comprise media streaming." Claim 25 recites similar, though not identical, features and operations. For disclosure of the recited elements, the Examiner relies on *Gudjonsson*. As discussed above with regard to independent Claim 1, however, *Gudjonsson* is limited to a network for routing incoming communications to an appropriate device based upon the type of communication. Thus, the disclosure of *Gudjonsson* is focused on the set up of the communication as it is initially received. Although *Gudjonsson* disclose the maintaining of an event log, the monitoring of login status by users, and the user of a firewall, these functions do not result in "monitoring the telecommunication link" as recited in dependent Claims 9-10 and 24-25. Rather, the functions of the system of *Gudjonsson* merely operate to identify and prevent hacking to the system. As such, *Gudjonsson* cannot be said to disclose, teach, or suggest monitoring the telecommunication link to determine whether the telecommunications being sent by the untrusted device use "an appropriate audio format" or "comprise media streaming." These features and operations are completely absent from the teachings of *Gudjonsson*.

For at least these reasons, the rejection of Claims 2-13, 14, and 17-45 should be withdrawn. Therefore, Applicants respectfully request reconsideration and allowance of Claims 2-13, 14, and 17-45.

## CONCLUSION

Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully requests full allowance of all pending claims.

If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the Examiner is invited to contact Jenni R. Moen, Attorney for Applicants, at the Examiner's convenience at (214) 953-6809.

Although no fees are believed to be due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Jenni R. Moen

Jenni R. Moen
Reg. No. 52,038

Date: February 17, 2005

**Correspondence Address:**

Customer No. **05073**